

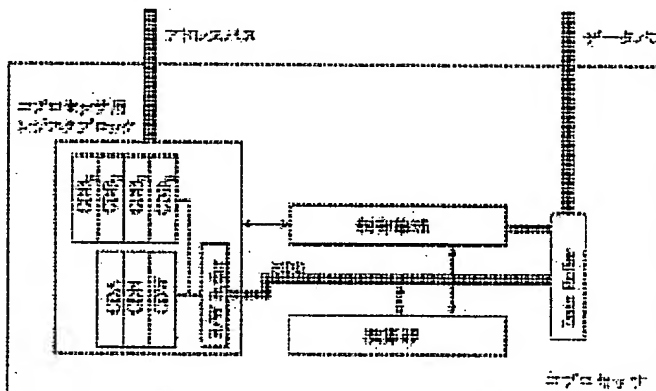
IC CARD AND MICROCOMPUTER**Publication number:** JP2001195555 (A)**Publication date:** 2001-07-19**Inventor(s):** TERAUCHI CHIAKI; NAKADA KUNIHICO; TSUKAMOTO TAKU;
WATASE HIROSHI**Applicant(s):** HITACHI LTD; HITACHI ULSI SYS CO LTD**Classification:****- international:** G06F12/14; G06F21/24; G06K19/07; G09C1/00; G06F12/14;
G06F21/00; G06K19/07; G09C1/00; (IPC1-7): G06K19/07;
G06F12/14; G09C1/00**- European:****Application number:** JP20000003297 20000112**Priority number(s):** JP20000003297 20000112**Also published as:**

JP4168305 (B2)

Abstract of JP 2001195555 (A)

PROBLEM TO BE SOLVED: To provide an IC card and a microcomputer, for which the strengthening of secrecy protection is realized. **SOLUTION:**

Concerning the IC card or microcomputer in module configuration provided with the input/output operation of data accompanied with enciphering or deciphering processing by an arithmetic unit for cipher processing to be operated by supplying an operating voltage by electrically connecting an external terminal with a reader/writer and receiving an instruction from a central processing unit, the arithmetic unit for cipher processing is provided with a register for storing data to be used for operation for enciphering or deciphering processing for the unit of plural bits and before enciphering or deciphering processing, the required data are fetched into such a register.



Data supplied from the esp@cenet database — Worldwide

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2001-195555

(P2001-195555A)

(43)公開日 平成13年 7月19日 (2001. 7. 19)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)	
G 0 6 K 19/07		G 0 6 F 12/14	3 2 0 B	5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 9 C 1/00	6 2 0 B	5 B 0 3 5
G 0 9 C 1/00	6 2 0		6 5 0 A	5 J 1 0 4
	6 5 0		6 6 0 A	9 A 0 0 1
	6 6 0	G 0 6 K 19/00	N	
審査請求 未請求 請求項の数13 O L (全 18 頁)				

(21)出願番号 特願2000-3297(P2000-3297)

(22)出願日 平成12年 1月12日 (2000. 1. 12)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(71)出願人 000233169

株式会社日立超エル・エス・アイ・システムズ

東京都小平市上水本町 5 丁目22番 1 号

(72)発明者 寺内 千晶

東京都小平市上水本町五丁目20番 1 号 株式会社日立製作所半導体グループ内

(74)代理人 100081938

弁理士 徳若 光政

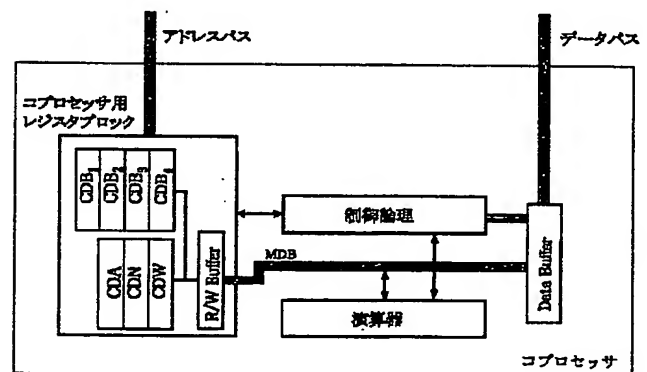
最終頁に続く

(54)【発明の名称】 I Cカードとマイクロコンピュータ

(57)【要約】

【課題】 機密保護の強化を実現した I Cカードとマイクロコンピュータを提供する。

【解決手段】 外部端子がリードライト装置と電氣的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含む I Cカード又はモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータをかかえるレジスタに取り込むようにする。



【特許請求の範囲】

【請求項 1】 外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含む IC カードであって、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに格納してなることを特徴とする IC カード。

【請求項 2】 請求項 1 において、上記暗号化処理又は復号化処理は、RSA 暗号法などに应用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力された X、Y 及び N を受け、 $A = 1$ 、 $B = X$ として、 $A = A^2 \bmod N$ と $A = AB \bmod N$ の演算を交互に行ない、かかる演算において Y の上位から複数ビットずつみて、上記複数ビットに対応した $A = A^2 \bmod N$ の演算を行ない、複数ビットの組み合わせに対応して $AB \bmod N$ の演算に必要な B の値を上記レジスタから取り込むものであることを特徴とする IC カード。

【請求項 3】 外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含む IC カードであって、上記暗号処理用演算ユニットは、暗号化処理又は復号化処理のための演算動作と並行して次の演算に使用するデータを記憶回路から取り込む信号経路を有することを特徴とする IC カード。

【請求項 4】 請求項 3 において、上記暗号化処理又は復号化処理は、RSA 暗号法などに应用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力された X、Y 及び N を受け、 $A = 1$ 、 $B = X$ として、 $A = A^2 \bmod N$ と $A = AB \bmod N$ の演算を交互に行ない、かかる演算において Y の上位から複数ビットずつみて、上記複数ビットに対応した $A = A^2 \bmod N$ の演算を行ない、かかる演算と並行して複数ビットの組み合わせに対応した $AB \bmod N$ の演算に必要な B の値を上記記憶回路から取り込むものであることを特徴とする IC カード。

【請求項 5】 外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含む IC カードであって、上記中央処理装置は、暗号化又は復号化処理のためのデ

ータが格納された先頭アドレスを上記記憶回路に供給し、上記記憶回路は上記先頭アドレスを基に内蔵されたアドレス発生回路により形成されたアドレス信号に基づいてデータを読み出して上記暗号処理用演算ユニットにデータ転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスには乱数発生回路で形成された乱数が偽アドレス信号として送出されるものであることを特徴とする IC カード。

【請求項 6】 請求項 5 において、上記暗号化処理又は復号化処理は、RSA 暗号法などに应用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力された X、Y 及び N を受け、 $A = 1$ 、 $B = X$ として、 $A = A^2 \bmod N$ と $A = AB \bmod N$ の演算を交互に行ない、かかる演算において Y の上位から複数ビットずつみて、上記複数ビットに対応した $A = A^2 \bmod N$ の演算を行ない、上記複数ビットの組み合わせに対応して $AB \bmod N$ の演算に必要な B の値を上記記憶回路から取り込むものであることを特徴とする IC カード。

【請求項 7】 外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含む IC カードであって、上記中央処理装置は、上記乱数発生回路で形成された乱数を用いて形成された暗号化されたアドレス信号を上記記憶回路に供給し、記憶回路では上記乱数を用いて上記アドレス信号を復号化して先頭アドレスを生成し、上記記憶回路は、上記先頭アドレスを基に内蔵されたアドレス発生回路により形成されたアドレス信号に基づいて暗号化処理又は復号化処理のためのデータを読み出して上記暗号処理用演算ユニットに転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスには上記乱数発生回路で形成された乱数が偽アドレス信号として送出されるものであることを特徴とする IC カード。

【請求項 8】 請求項 7 において、上記暗号化処理又は復号化処理は、RSA 暗号法などに应用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力された X、Y 及び N を受け、 $A = 1$ 、 $B = X$ として、 $A = A^2 \bmod N$ と $A = AB \bmod N$ の演算を交互に行ない、かかる演算において Y の上位から複数ビットずつみて、上記複数ビットに対応した $A = A^2 \bmod N$ の演算を行ない、上記複数ビットの組み合わせに対応して $AB \bmod N$ の演算に必要な B の値を上記記憶回路から取り込むものである

ことを特徴とする IC カード。

【請求項 9】 中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータであって、

上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに格納してなることを特徴とするマイクロコンピュータ。

【請求項 10】 請求項 9 において、

上記モジュール構成は、1つの半導体基板上において形成されることによって実現されることを特徴とするマイクロコンピュータ。

【請求項 11】 中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータであって、

上記暗号処理用演算ユニットは、暗号化処理又は復号化処理のための演算動作と並行して次の演算に使用するデータを記憶回路から取り込む信号経路を有することを特徴とするマイクロコンピュータ。

【請求項 12】 中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータであって、

上記中央処理装置は、暗号化又は復号化処理のためのデータが格納された先頭アドレスを上記記憶回路に供給し、

上記記憶回路は上記先頭アドレスを基に内蔵されたアドレス発生回路により形成されたアドレス信号に基づいてデータを読み出して上記暗号処理用演算ユニットにデータ転送し、

上記乱数発生回路は、上記データ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスに生成した乱数を偽アドレス信号として送出することを特徴とするマイクロコンピュータ。

【請求項 13】 中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータであって、

上記中央処理装置は、上記乱数発生回路で形成された乱数を用いて形成された暗号化されたアドレス信号を上記記憶回路に供給し、

上記記憶回路は、上記中央処理装置から供給された上記

暗号化されたアドレス信号を上記乱数を用いて復号化して先頭アドレスを生成し、暗号化処理又は復号化処理のためのデータを読み出して上記暗号処理用演算ユニットに転送し、

上記乱数発生回路は、上記データ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスに生成した乱数を偽アドレス信号として送出することを特徴とするマイクロコンピュータ。

10 【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、IC カードとマイクロコンピュータに関し、特に IC カードやプログラム内蔵の 1 チップマイクロコンピュータのような CPU とメモリを含み暗号鍵を使ったデータ処理を行なうものの機密保護技術に利用して有効な技術に関するものである。

【0002】

【従来の技術】メモリに保存されている鍵情報を用いてデータの暗号化処理又は復号化処理を行なうようにした IC カードにおいて、処理時間の違いを利用して実行内容や暗号鍵を推定する TA (Timing Attack) 法のようなハッキング手法に対抗するため、暗号処理化又は復号化処理の実行中又は実行の前後に、鍵情報の内容との時間的な相関関係を喪失させる遅延処理を実行する技術の例として、特開平 10-69222 号がある。また、IC カードに関しては、オーム社出版電子情報通信学会編水沢順一著「IC カード」などがある。

【0003】

【発明が解決しようとする課題】近年、IC カードが暗号処理を行っている時の消費電流を観測して解析することにより、容易に暗号処理の内容や暗号鍵が推定されることの可能性が示唆されている。このことについては、John Wiley & sons 社 W. Rankl & W. Effing 著「Smart Card Handbook」の 8.5.1.1 Passive protective mechanisms (263 ページ) に記載されている。

【0004】つまり、SPA (Simple Power Analysis) 法では、演算命令の違い、あるいは処理されているデータの違いにより生じる消費電流波形の違いから、暗号鍵や処理されているデータを解析し、DPA (Differential Power Analysis) 法では、消費電流波形を統計処理して暗号鍵を推定する。この DPA 法では、例えば DES のある部分に仮定した暗号鍵をあてはめて、平文を変化させながら消費電流波形を測定して統計する。暗号鍵を様々に変化させながらこの作業を繰り返し、正しい鍵のときには電流波形が大きなピークを示す。

【0005】前記公報に記載のように TA (Timing Attack) 法のみを考慮した遅延処理では、実際の演算による消費電流の相関性までも喪失させることができず、上記のような消費電流波形を観測するという SPA 又は D

PA法のようなハッキング手法には対抗できない。そこで、本願発明者等においては、上記ICカード及びICカード等のようなモジュールに搭載されるマイクロコンピュータのように内蔵のプログラムにより一定のデータ処理動作を行うものに対して上記のような消費電流の観測による暗号処理の内容や暗号鍵の解読をより確実に防止することができる機密保護技術を開発するに至った。

【0006】この発明の目的は、機密保護の強化を実現したICカードとマイクロコンピュータを提供することにある。この発明の前記ならびにそのほかの目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【0007】

【課題を解決するための手段】本願において開示される発明のうち代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むICカードにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータをかかえるレジスタに取り込むようにする。

【0008】本願において開示される発明のうち他の代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに取り込むようにする。

【0009】

【発明の実施の形態】図1には、この発明が適用されるICカードの一実施例の外観図が示されている。ICカードは、プラスチックケースからなるカード101と、かかるカード101の内部に搭載された図示しない1チップのマイクロコンピュータ等からなるICカード用チップを持つものである。上記ICカードは、さらに上記ICカード用チップの外部端子に接続されている複数の接点(電極)102を持つ。複数の接点102は、後で図2によって説明するような電源端子VCC、電源基準電位端子VSS、リセット入力端子RESバー、クロック端子CLK、データ端子I/O-1/I/RQバー、I/O-2/I/RQバーとされる。ICカードは、かかる接点102を通して図示しないリーダーライタのような外部結合装置から電源供給を受け、また外部結合装置と

の間でのデータの通信を行う。

【0010】図2には、この発明に係るICカードに搭載されるICカード用チップ(マイクロコンピュータ)の一実施例の概略ブロック図が示されている。同図の各回路ブロックは、公知のMOS集積回路の製造技術により、特に制限されないが、単結晶シリコンのような1個の半導体基板上において形成される。

【0011】この発明に係るICカード用チップの構成は、基本的にマイクロコンピュータと同じような構成である。その構成は、クロック生成回路205、中央処理装置(以下単にCPUという場合がある)201、ROM(Read Only Memory)206やRAM(Random Access Memory)207、不揮発性メモリ208などの記憶装置、暗号化及び復号化処理の演算を行なうコプロセッサ209、入出力ポート(I/Oポート)202などからなる。

【0012】クロック生成回路205は、図示しないリーダーライタ(外部結合装置)から図1の接点102を介して供給される外部クロックCLKを受け、かかる外部クロック信号に同期したシステムクロック信号を形成し、それをチップ内部に供給する回路である。CPU201は、論理演算や算術演算などを行う装置であり、システムコントロールロジック、乱数発生器及びセキュリティロジック及びタイマなどを制御する。記憶装置206、207、208は、プログラムやデータを格納する装置である。コプロセッサ209は、後述するようにRSA暗号法などに応用可能なべき乗剰余乗算動作を行なう演算器とレジスタ及び制御論理から構成される。I/O(入出力)ポート202は、リーダーライタと通信を行う装置である。データバス204とアドレスバス203は、各装置を相互に接続するバスである。

【0013】上記記憶装置206、207、208のうち、ROM206は、記憶内容が不揮発的に固定されているメモリであり、主にプログラムを格納するメモリである。揮発性メモリ(以下、RAMという)207は自由に記憶情報の書き換えができるメモリであるが、電源の供給が中断されると、記憶している内容が消えてなくなる。ICカードがリーダーライタから抜かれると電源の供給が中断されるため、RAM207の内容は、保持されなくなる。

【0014】上記不揮発性メモリ(以下、EEPROM(Electrical Erasable Programmable Read Only Memory)という)208は、内容の書き換えが可能な不揮発性メモリであり、その中に一旦書き込まれた情報は、電源の供給が停止されてもその内部に保持される。このEEPROM208は、書き換える必要があり、かつICカードがリーダーライタから抜かれても保持すべきデータを格納するために使われる。例えば、ICカードがプリペイドカードとして使用されるような場合、のプリペイドの度数などは、使用するたびに書き換えられる。この

場合の度数などは、リーダーライトが抜かれても IC カード内で記憶保持する必要があるため、EEPROM 208 で保持される。

【0015】CPU 201 は、いわゆるマイクロプロセッサと同様な構成にされる。すなわち、その詳細を図示しないけれども、その内部に命令レジスタ、命令レジスタに書込まれた命令をデコードし、各種のマイクロ命令ないしは制御信号を形成するマイクロ命令 ROM、演算回路、汎用レジスタ (RG 6 等)、内部バス BUS に結合するバスドライバ、バスレシーバなどの入出力回路を持つ。CPU 201 は、ROM 206 などに格納されている命令を読み出し、その命令に対応する動作を行う。CPU 201 は、I/O ポート 202 を介して入力される外部データの取り込み、ROM 206 からの命令や命令実行のために必要となる固定データのようなデータの読み出し、RAM 207 や EEPROM 208 に対するデータの書き込みと読み出し動作制御等を行う。

【0016】上記 CPU 201 は、クロック生成回路 205 から発生されるシステムクロック信号を受けそのシステムクロック信号によって決められる動作タイミング、周期をもって動作される。CPU 201 は、その内部の主要部が P チャンネル型 MOSFET と N チャンネル型 MOSFET とからなる CMOS 回路から構成される。特に制限されないが、CPU 201 は、CMOS スタティックフリップフロップのようなスタティック動作可能な CMOS スタティック回路と、信号出力ノードへの電荷のプリチャージと信号出力ノードへの信号出力とをシステムクロック信号に同期して行うような CMOS ダイナミック回路とを含む。

【0017】IC カードのセキュリティ機能としては、チップ内部で乱数を自動生成する乱数発生器や、ランダムに割込みを生成するタイマー機能などの他に、本願発明にかかる高セキュリティ機能として、IC カードと外部装置とのデータ送受信の際に用いる RSA 暗号法などに応用可能なべき乗剰余演算動作を行なう暗号処理用演算ユニット (コプロセッサ) 209 を内蔵している。このコプロセッサ 209 は専用のレジスタが内蔵されている。

【0018】IC カードにおけるセキュリティ・システムでは、通信データの暗号処理は必須であり、この実施例でも現在最も多く利用されている公開鍵暗号として RSA 暗号が用いられる。この暗号法では、暗号化・復号化ともにべき乗剰余乗算 $X^Y \bmod N$ を用いるが、これは公知の Montgomery 法といわれる計算アルゴリズムによって剰余乗算 $A^2 \bmod N$ と $AB \bmod N$ の 2 つの形に分解することができる。つまり、 $Y = e_n \cdot e_{n-1} \cdots e_1$ の値 e_i を上位 e_n から最下位の e_1 まで順に 1 ビットずつ見ていき、 $e_i = 0$ だったら $A^2 \bmod N$ のみを、 $e_i = 1$ だったら $A^2 \bmod N$ と $AB \bmod N$ を演算する。したがって、 $e_i = 0$ のときには $A^2 \bmod N$

の演算の後に $i = 0$ であるかの判定処理が行なわれ、 $e_i = 1$ のときには $A^2 \bmod N$ と $AB \bmod N$ との演算の後に $i = 0$ であるかの判定処理が行なわれるために、 $e_i = 0$ と 1 とに対応した 2 通りの電流波形の形態が現れてしまう。

【0019】この実施例のようにコプロセッサ 209 を用いた場合には、その消費電流は CPU の消費電流に比べて比較的大きいため、この部分の電流波形を観測することによりコプロセッサの動作形態を比較的容易に識別することができ、前記 TA 法と SPA 法により暗号鍵 Y の値をハッキングされてしまう可能性が高い。そこで、この実施例のコプロセッサ 209 では、上記暗号化・復号化ともに用いられるべき乗剰余乗算 $X^Y \bmod N$ の演算を行なうに当たり攪乱目的のダミーの演算が挿入される。つまり、図 3 のタイミング図及び図 4 のフローチャート図に示すように $e_i = 0$ でも 1 でも $A^2 \bmod N$ と $AB \bmod N$ の両方の演算を常に行なうようにするものである。

【0020】図 3 のタイミング図において、(a) に示すように本来は、 $e_n = 1$ のときには $A^2 \bmod N$ の演算を行い、 e_n の判定の 1 により時間 t_1 を経て $AB \bmod N$ の演算を行い、その演算後に i をデクリメント ($n-1$) して $i = 0$ の判定に時間 t_2 を費やす。次いで、次ビット $e_{n-1} = 0$ のときは、 $A^2 \bmod N$ の演算を行い、 $e_{n-1} = 0$ の判定と i をデクリメント ($n-2$) して $i = 0$ の判定に時間 t_3 を費やす。そして、次ビット $e_{n-2} = 1$ のときには、 $A^2 \bmod N$ の演算を行い、 e_{n-2} の判定の 1 により時間 t_1 を経て $AB \bmod N$ の演算を行い、その演算後に i をデクリメント ($n-3$) して $i = 0$ の判定に時間 t_2 を費やす。以下、同様に e_i まで同様な動作を繰り返すものである。

【0021】この実施例のコプロセッサ 209 においては、上記暗号鍵 Y の各ビット e_i の論理 0 又は 1 に無関係に $A^2 \bmod N$ の演算の後に $AB \bmod N$ の演算を行なうようにする。図 3 (b) の $e_{n-1} = 0$ のときのように e_i が論理 0 のときにおける上記 $AB \bmod N$ の演算が攪乱目的のダミー演算として挿入される。つまり、

(b) のタイミング図及び図 4 のフローチャート図のように、 $A^2 \bmod N$ と $AB \bmod N$ の演算動作の間には、例えば e_i の判定の判定を含む時間 t_1 が費やされ、 $AB \bmod N$ と次ビットに対応した $A^2 \bmod N$ の演算動作の間には、 i のデクリメント動作と $i = 0$ の判定時間 t_2 が費やされる画一化された動作タイミング及び動作電流とすることができる。ただし、この実施例では、 e_i の判定処理は、その結果が演算動作の分岐の条件とされないため図 4 のフローチャート図では省略されている。

【0022】図 5 には、上記コプロセッサの一実施例のブロック図が示されている。この実施例では、主に演算器、制御論理、専用レジスタブロックより構成され、ベ

き乗剰余演算の最終結果はデータバッファ、データバスを介して中央処理装置CPUに送信される。専用レジスタは、アドレスバスから供給されるアドレス信号に対応してその選択動作が行なわれる。

【0023】この実施例では、内部バスMDBとレジスタブロックのリードライトバッファ(R/W Buffer)との間にゲート回路1が設けられる。このゲート回路1は、制御論理により制御が行なわれて、 e_i が論理0ならば $A^2 \bmod N$ 動作の演算結果が内部バスMDBとリードライトバッファを介して所定のレジスタCDAに取り込まれた後開いていたゲートが閉じるようにされる。つまり、上記演算結果がリードライトバッファに取り込まれると、その後にゲートを閉じてしまいリードライトバッファへの新たなデータの書き込みを禁止する。したがって、その後に行なわれる $AB \bmod N$ の演算結果は無効データとして扱われることとなる。また、 e_i が論理1ならばゲート回路1はゲートを開いた状態のままとされる。

【0024】図6には、上記コプロセッサの他の一実施例のブロック図が示されている。この実施例では、レジスタブロックのリードライトバッファ(R/W Buffer)と各レジスタとの間にゲート回路2が設けられる。このゲート回路2は、前記同様に制御論理により制御が行なわれて、 e_i が論理0ならば $A^2 \bmod N$ 動作の演算結果が内部バスMDBとリードライトバッファとを介して所定のレジスタCDAに書き込まれた後に開いていたゲートが閉じるようにされる。つまり、上記演算結果がレジスタCDAに取り込まれると、その後にゲートを閉じてしまいかかるレジスタCDAへの新たなデータの書き込みを禁止する。したがって、その後に行なわれる $AB \bmod N$ の演算結果は、リードライトバッファまでは書き込まれるが、実際には無効データとして扱われることとなる。また、 e_i が論理1ならばゲート回路2はゲートを開いた状態のままとされる。

【0025】図7には、上記ゲート回路の一実施例の内部構成図が示されている。ダミー書き込み制御ユニットは、アンドゲート回路によって構成され、一方の入力には制御論理からのライトイネーブル信号が供給され、他方の入力には演算器で生成されたライトストロープ信号が供給される。上記ゲート回路の出力信号は、データバッファ(R/W Buffer)と専用レジスタにライトストロープ信号として伝えられる。

【0026】この実施例では、演算結果そのものの伝達制御するものに代えて、レジスタ又はデータバッファへの書き込み動作を指示するライトストロープ信号の発生タイミングを切り換えるようにするものである。つまり、 $e_i = 0$ のときには、 $A^2 \bmod N$ 動作の演算結果が出力された後にライトイネーブル信号をロウレベルとしてアンドゲート回路のゲートが閉じるようにするものである。逆に、 $e_i = 1$ のときには、制御論理はライト

イネーブル信号をハイレベルのままとして、演算器で形成されたライトストロープ信号がそのままデータバッファ又は専用レジスタに伝えられる。この構成では、複数ビットからなる演算結果Aに対応して、複数個のゲート回路を設ける必要がないので簡素化が可能になる。

【0027】図8には、上記コプロセッサの他の一実施例のブロック図が示されている。この実施例では、レジスタブロックのリードライトバッファ(R/W Buffer)と各レジスタとの間にセクタ2とレジスタブロックにダミーレジスタ1が設けられる。このセクタ2は、前記同様に制御論理により制御が行なわれて、 e_i が論理0ならば $A^2 \bmod N$ 動作の演算結果が内部バスMDBとリードライトバッファとを介して所定のレジスタCDAに書き込まれるような信号経路を形成し、その後にダミーレジスタ1を選択するような信号経路を形成する。

【0028】つまり、上記演算結果がレジスタCDAに取り込まれると、その後にダミーレジスタ1を選択するので、レジスタCDAへの新たなデータの書き込みを禁止しつつその後に行なわれる $AB \bmod N$ の演算結果がダミーレジスタに書き込まれものとなる。 e_i が論理1ならばセクタ2は常にレジスタCDAを選択する。この構成は、演算結果をレジスタに書き込む動作を含めて e_i が論理0のときと論理1のときとで電流波形で見たときに全く同一にすることができるから、電流波形を利用したアタックをより確実に無力化することができる。

【0029】図9には、この発明に係るコプロセッサの他の一実施例の動作を説明するための構成図が示されている。図9(a)のタイミング図及び(b)のフローチャート図において、前記説明したように、 $A^2 \bmod N$ の演算後、 e_i の判定の時間 t_1 の間もダミー演算動作として $A^2 \bmod N$ を継続して $AB \bmod N$ の演算に移行する。

【0030】その演算後に i をデクリメント (-1) して $i = 0$ の判定に時間 t_2 を費やすが、その間も上記 $AB \bmod N$ の演算を継続させる。以下、同様に e_i まで同様な動作を繰り返すものである。この構成は、演算動作中は、 e_i が論理0と1のときに関係なく上記のような演算動作を継続するので、電流波形で見たときに格別な特徴を見出すことができないから、電流波形を利用したアタックを無力化することができる。

【0031】図10には、図9のコプロセッサの動作を実現するための一実施例のブロック図が示されている。制御論理では、ダミーイネーブル信号とコプロイネーブル信号を送出する。上記ダミーイネーブル信号とコプロイネーブル信号は、オアゲート回路を通して演算器に入力される。それ故、コプロイネーブル信号がアクティブであるときに加えて、ダミーイネーブル信号がアクティブであるときにも演算器は演算動作を行なうようにされる。

【0032】上記ダミーイネーブル信号は、インバータ回路を通してアンドゲート回路の一方の入力に供給され、かかるアンドゲート回路の他方の入力には演算器で形成されたライトストロブ信号が供給される。つまり、演算器で形成されたライトストロブ信号の伝達をダミーイネーブル信号で選択的に停止できるようにする。コプロイネーブル信号がアクティブにされて、前記正規の演算動作が終了すると、その演算結果を出力するためのライトストロブ信号が形成される。このようにコプロイネーブル信号がアクティブのときには、ダミーイネーブル信号の反転信号がアクティブレベルとなってアンドゲート回路のゲートを開くように制御するので、上記正規演算結果はライトストロブ信号によって、R/Wバッファ又はレジスタブロックの所定のレジスタに書き込まれる。

【0033】上記のような正規演算が終了すると、ダミーイネーブル信号がアクティブとなって演算器に対して演算動作を指示する。この演算の終了によって、上記ライトストロブ信号が形成されるが、上記ダミーイネーブル信号の反転信号によってアンドゲート回路がゲートを閉じているので、上記攪乱目的のダミー演算動作によって発生されたライトストロブ信号がR/Wバッファ又はレジスタブロックの所定のレジスタに伝えられることはない。これにより、攪乱目的のダミー演算結果は無効データとして消失させられる。

【0034】図11には、この発明に係るコプロセッサの他の一実施例の動作を説明するためのタイミング図が示されている。前記図3に示した実施例のように、攪乱目的のダミー演算を挿入して、(a)のタイミング図のように、 e_i に対して画一化して $A^2 \bmod N$ と $AB \bmod N$ の演算を一対として行なうようにした場合でも、各演算には、演算結果にオーバーフロー処理を必要とするもの(あり)のものと、オーバーフロー処理を必要としないもの(なし)が発生する。

【0035】このようなオーバーフロー処理は、演算時間を長くするものであるので電流波形でみると、オーバーフロー処理ありとなしとの識別が可能になる。このような電流波形の特徴から演算内容や演算データを推測することも不可能ではないと考えられるため、この実施例では(b)のタイミング図に示すようにオーバーフロー処理を不要とする演算に対しても必要なときと同様にオーバーフロー処理を挿入する。つまり、みかけ上は、全ての演算 $A^2 \bmod N$ と $AB \bmod N$ の演算において画一的にオーバーフロー処理のための動作が実施されるために、その識別を無力化するものである。

【0036】図12は、この発明に係るコプロセッサの他の一実施例の動作を説明するためのフローチャート図が示されている。このフローチャート図は、前記図11(b)に対応している。 $A^2 \bmod N$ と $AB \bmod N$ の各演算は、剰余演算部とオーバーフロー演算部からな

り、演算結果に無関係に上記オーバーフロー演算処理を実施するものである。

【0037】図13には、この発明に係るコプロセッサの他の一実施例の動作の詳細を説明するためのタイミング図が示されている。この実施例による対策前では、前記 $A^2 \bmod N$ と $AB \bmod N$ のようなコプロ演算においては、その演算結果に対応してオーバーフロー処理のあるものと無いもの2種類が存在したが、この実施例による対策後では、前記 $A^2 \bmod N$ と $AB \bmod N$ のようなコプロ演算においては、その演算結果に無関係に常にオーバーフロー処理が実行される。このため、本来はオーバーフロー処理が不要な演算動作に対して実施されたオーバーフロー処理は、攪乱目的のダミー動作とされる。

【0038】図14には、図11ないし図13に示したコプロセッサの動作を実現するための一実施例のブロック図が示されている。制御論理では、ダミーオーバーフロー信号とコプロオーバーフロー信号を送出する。上記ダミーオーバーフロー信号とコプロオーバーフロー信号は、オアゲート回路を通して演算器に入力される。それ故、コプロオーバーフロー信号がアクティブであるときに加えて、ダミーオーバーフロー信号がアクティブであるときにも演算器はオーバーフロー処理動作を行なうようにされる。

【0039】上記コプロオーバーフロー信号は、アンドゲート回路の一方の入力に供給され、かかるアンドゲート回路の他方の入力に演算器で形成されたライトストロブ信号が供給される。つまり、演算器で形成されたライトストロブ信号の伝達をコプロオーバーフロー信号がアクティブレベルでないときに選択的に停止できるようにする。つまり、コプロオーバーフロー信号がアクティブレベルでないときはダミーオーバーフロー信号によって演算器がオーバーフロー処理を行なっているので、かかるオーバーフロー処理で形成されたライトストロブ信号は上記ゲート回路のゲートを閉じることによって無効にするものである。したがって、前記正規のオーバーフロー処理終了すると、その処理結果を出力するためのライトストロブ信号が形成されて、R/Wバッファ又はレジスタブロックの所定のレジスタに処理結果が書き込まれる。

【0040】これに対して、ダミーオーバーフロー信号がアクティブとなって演算器に対してオーバーフロー処理動作を指示した場合には、そのオーバーフロー処理によって形成されたライトストロブ信号は、上記コプロオーバーフロー信号によってアンドゲート回路のゲートが閉じられるものであるから、上記攪乱目的のダミーオーバーフロー処理動作によって発生されたライトストロブ信号がR/Wバッファ又はレジスタブロックの所定のレジスタに伝えられることはない。これにより、攪乱目的のダミーオーバーフロー処理結果は無効データとし

て消失させられる。

【0041】図15には、この発明に係るコプロセッサの更に他の一実施例の動作を説明するためのタイミング図が示されている。(a)に示すように本来は、 $e_n = 1$ のときには $A^2 \bmod N$ の演算を行い、 e_n の判定の1により時間 t_1 を経て $AB \bmod N$ の演算を行い、その演算後に i をデクリメント($n-1$)して $i=0$ の判定に時間 t_2 を費やす。次いで、次ビット $e_{n-1} = 0$ のときは、 $A^2 \bmod N$ の演算を行い、 e_{n-1} の判定と i をデクリメント($n-2$)して $i=0$ の判定に時間

【0042】(b)のタイミング図では、上記攪乱目的のダミーサイクルの挿入は、各演算毎の時間を最も長い時間 t_3 に揃えるように挿入するものである。これにより、時間 t_3 をインターバルとして $A^2 \bmod N$ 又は $AB \bmod N$ のいずれかの演算が実施されるために、みかけ上は演算動作に対応した電流波形が画一化されてその識別を無力化するものである。これに対して、(c)タイ

【0043】上記のような攪乱目的のダミーサイクルは、前記図2に示されたようにタイマーを利用して演算間隔を変更可変にするものである。あるいはコプロセッサの外部にタイマーを設けて一定の時間が経過するまで次の演算の実行を待つようにする。つまり、コプロセッサによるべき乗剰余乗算の演算において、図15(a)に示した前記各演算毎の時間 t_1 、 t_2 、 t_3 に攪乱目的のダミーのサイクルを挿入し、一定時間後にタイマーからの割込みを入れる。これにより、図15(b)に示すように t_1 、 t_2 、 t_3 の時間が全て一定となり、電流波形からの攻撃を困難にする。あるいはタイマーには乱数発生器で生成した乱数をセットしておき、(c)に示すように毎回 t_1 、 t_2 、 t_3 の時間をランダムに変化させることも可能である。また、タイマーを用いなくとも、ソフトウェアでカウントすることも可能である。

【0044】べき乗剰余乗算において、コプロセッサによる演算の高速化を目的とし、 Y の値を2ビット、あるいは3ビットずつ処理するようにすると、例えば図16のフローチャート図に示すように、2ビット処理の例で説明するなら常に $A^2 \bmod N - A^2 \bmod N - AB \bmod N$ 及び $i-2$ と $i=0$?の各ステップの繰り返しに

なるので、前記1ビットずつ行なう場合のような攪乱目的のダミー演算を行なわなくとも、処理時間や電流波形が一定になる。そのため、電流波形から Y の値を推定するのは困難になる。また演算の回数も、前記のバイナリ法だと最大で $2n$ 回かかっていたものを、2ビット処理だと常に $1.5n$ 回で済むために、動作時間の短縮にもつながる。

【0045】コプロセッサの演算が開始するまでに A 、 B 、 N の値をそれぞれコプロセッサ専用レジスタに転送し格納しておく。しかしながら、2ビット処理を行う場合、 Y の値によって4通りの B の値 B_1 、 B_2 、 B_3 、 B_4 が必要になり、これらの値は前もって計算して、RAMやEEPROMなどに格納しておき、毎回コプロセッサ専用レジスタに転送することになるが。この際、4通りの B の値によって転送中の電流波形に特徴が現れる可能性がある。

【0046】例えば、16ビットのプリチャージバスにデータを転送する場合を考える。プリチャージバスは、データ転送の前にすべてのバスの値を“1”にそろえるバスである。このバスに、値は違うが“1”のビットの数が同じデータ、例えば、“1”のビットの数が2である16進数で“88”と“11”、を転送した場合、電流波形はほぼ同じ波形になると予測される。この理由は、“1”から“0”へ変化したビットの数が同じであるため、同じように電流を消費し、同じ電流波形になるからである。

【0047】もし、“1”のビットの数が1つ異なるデータ、例えば、“1”のビットの数が3である“89”や“19”を転送した場合、“1”のビットの数が2のデータとは消費電流が異なる。これは、13ビット分バスの値が“1”から“0”に変わったため、その分の電流が消費される。そのため、先の14ビットが変化したデータに比べて消費電流が1ビット分小さくなる。一般に、変化するビットの数が多ほど電流波形は高くなるという規則性がある。この規則性から転送されているデータを推定することができると考えられる、電流アタックの対象となりやすい。これを防ぐため次のような工夫を行なうものである。

【0048】図17と図18には、この発明に係るコプロセッサの他の一実施例のブロック図がそれぞれ示されている。この実施例のコプロセッサは、2ビット処理と3ビット処理に向けられている。つまり、コプロセッサのレジスタ容量を増やして、2ビット処理の場合には4通りの B の値 $B_1 \sim B_4$ を、3ビット処理の場合には8通りの B の値 $B_1 \sim B_8$ をコプロセッサのレジスタに格納しておく。従って、演算の途中で記憶回路(RAM)からデータバスを通して上記コプロセッサのレジスタに前記のような転送の必要がなくなり、前記電流アタックに対して防御することができる。

【0049】つまり、前記図16に示したようなフロー

10

20

30

40

50

チャート図において、コプロセッサが $AB \bmod N$ を実行する際、下記のように4つ（3ビット処理のときにはあるいは8つ）のうちの正しいBレジスタCDBから値を選んで実行できるように、Yの2ビット（あるいは3ビット）の値をコプロセッサの制御レジスタ（CCN * 制御用レジスタ（CCNT）

ビット7	ビット6	ビット2	ビット1	ビット0
—	—			e_1	e_{1-1}

【0051】

演算の種類

ビット2	e_1	e_{1-1}	演算の種類
0	0	0	$A \leftarrow A^2 \bmod N$
0	1	0	$A \leftarrow A \bmod N$
0	1	1	$A \leftarrow A \times N$
1	0	0	$A \leftarrow AB_1 \bmod N$
1	0	1	$A \leftarrow AB_2 \bmod N$
1	1	0	$A \leftarrow AB_3 \bmod N$
1	1	1	$A \leftarrow AB_4 \bmod N$

【0052】図19には、この発明に係るコプロセッサの他の一実施例のブロック図が示されている。この実施例のコプロセッサも、2ビット処理や3ビット処理のような複数ビット処理に向けられている。この実施例では、データバスにスイッチを設けて演算をしながら転送できるようにする。この構成により、コプロセッサのレジスタ容量を増加させることなく、実行時間の短縮と電

流アタック対策の両方に効果的である。

【0053】コプロセッサ専用レジスタ（CDA, CDB, CDN, CDW）は、同図に示すように4つのレジスタがCPUとコプロセッサの演算器との間で排他的に使用されている。2ビット処理を行う場合、2回の $A^2 \bmod N$ を行いながらその間にBの値をRAMからコプロセッサ専用レジスタユニット中のBレジスタCDBに転送できるようにすると効率的である。

【0054】コプロセッサのAレジスタCDAとBレジスタCDBのI/Oを分け、それぞれにリード/ライトバッファ（R/W Buffer）を設けて、それぞれ独立に動作できるようにする。演算器が $A^2 \bmod N$ を演算している間は、制御信号によりデータバスをパス1（path 1）につなぎ、図示しないCPUのRAMからBの値を上記独立に設けられたリード/ライトバッファを介してBレジスタCDBに転送する。次に演算器が $AB \bmod N$ を実行する際には、制御信号によりパス2（path 2）に切り換え、上記BレジスタのB値を演算器に送り上記CPUがBレジスタCDBにアクセスできないようにする。この方法を取ると、 $A^2 \bmod N$ を演算動

* T) のビットに当てはめ、次に示す制御レジスタ及び演算の種類のように、2ビット処理の場合には、 $AB_1 \bmod N$, $AB_2 \bmod N$, $AB_3 \bmod N$, $AB_4 \bmod N$ のうちどの演算をするかを選択させるようにする。

【0050】

作と、B値の転送動作が同時に行なわれるから演算時間が短縮されるだけでなく、演算と転送の消費電流が重なるため双方の波形が識別できなくなり、電流アタック対策に有効である。

【0055】図20には、この発明に係るICカード用チップの他の一実施例の要部ブロック図が示されている。この実施例では、暗号処理用演算ユニットとメモリ（RAM）間の転送の際、メモリにカウンタを設けるようにするものである。この実施例では、2ビット処理に用いる4通りの値、あるいは3ビット処理に用いる8通りの値をコプロセッサ外部メモリRAMからコプロセッサ専用レジスタユニット中のBレジスタCDBに転送する際の電流攪乱を行なうようにするものである。

【0056】この実施例では、前記図2に示したようなICカード用チップにおいて、RAMの側にカウンタが設けられる。RAMは、カウンタで形成されたアドレス信号をデコードしてデータをデータバスに送出する。このとき、アドレスバスには、乱数発生器が形成された偽アドレスが送出される。これにより、アドレスとデータとの相関が無くなり、電流解析を無力化させることができる。

【0057】図21には、上記カウンタの一実施例のブロック図が示されている。カウンタは、転送したいブロックの最初のアドレスを保持する先頭アドレスレジスタとインクリメントを用い、ブロック転送をイネーブルにするイネーブル信号とクロック又はリード/ライト信号などによるインクリメント指示信号で制御する。ブロッ

30

40

50

ク転送を開始する際、まず転送の先頭アドレスと転送開始のイネーブル信号がCPUよりカウンタに送信され、上記先頭アドレスレジスタに保持される。その後は、インクリメント指示信号によって、インクリメントが動作して先頭アドレスレジスタの先頭アドレスA+1を形成して、アドレスを生成するとともに上記先頭アドレスレジスタの内容を書き換えるので、図22のタイミング図に示すように、RAMアドレスが順番にインクリメントA、A+1、A+2、・・・されていき、そのアドレスに従って順次データD_A、D_{A+1}、D_{A+2}・・・が書

込まれ/読み出される。
 【0058】この実施例では、ブロック転送がイネーブルになった後はアドレスバスからのアドレスをカウンタが受け付けられないため、アドレスバスにどのような値が来ようとデータは正しく読み出されていく。従って、アドレスバスに乱数発生器などで生成した乱数B、C、D、E・・・が出力されるとアドレスバスの消費電流を攪乱でき、この効果からチップ全体の消費電流を攪乱できるため、チップ内部動作の解析を困難にすることが可能になる。

【0059】図23には、この発明に係るICカード用チップの更に他の一実施例を示す要部ブロック図が示されている。この実施例でも、暗号処理用演算ユニットとメモリ(RAM)間の転送の際、メモリにカウンタを設けるようにするものであるが、かかる暗号処理用演算ユニットとメモリRAMの最初のアドレスをも攪乱するようアドレスオフセット機能が設けられる。つまり、乱数発生器などで生成した乱数をあらかじめCPUとカウンタ側に同時に転送しておき、ブロック転送の最初のアドレスに乱数を加えるか又は引くかした値をアドレスバスに出力する。カウンタ側ではアドレスバスの値を同じ乱数を用いて復号化し、最初のアドレスを得る。

【0060】図24には、上記転送動作を説明するためのタイミング図が示されている。乱数発生器で形成された乱数をあらかじめCPUとRAMに転送しておき、オフセット演算部1によりブロック転送の最初のアドレスAに乱数Sを加えるか引くかしたアドレスA±Sをアドレスバスに送出する。カウンタ側では、アドレスバスの値を同じ乱数Sを用いて復号化し、オフセット演算部2により最初のアドレスAを得て、以後前記同様にインクリメントしてアドレスA+1、A+2・・・を生成する。このようなアドレスA+1、A+2に同期して、乱数発生器が乱数B、C、D・・・をアドレスバスに送出するので、先頭のアドレスを含めてアドレスバスの消費電流を攪乱でき、チップ内部動作の解析をいっそう困難にすることが可能になる。

【0061】上記の実施例から得られる作用効果は、下記の通りである。すなわち、

(1) 外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理

装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むICカードにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータにかかるレジスタに取り込むようにすることにより、演算動作の過程でのデータ転送を無くすことができるから、電流波形でのハッキングを無力化することができるという効果が得られる。

【0062】(2) 上記に加えて、上記暗号化処理又は復号化処理を、RSA暗号法などに応用可能なべき乗剰余乗算動作を含むものとし、上記暗号化処理用演算ユニットは、入力されたX、Y及びNを受け、 $A=1$ 、 $B=X$ として、 $A=A^2 \bmod N$ と $A=AB \bmod N$ の演算を交互に行ない、かかる演算においてYの上位から複数ビットずつみて、上記複数ビットに対応した $A=A^2 \bmod N$ の演算を行ない、複数ビットの組み合わせに対応して $AB \bmod N$ の演算に必要なBの値を上記レジスタから取り込むことにより、暗号処理の高速化と機密保護とを実現できるという効果が得られる。

【0063】(3) 外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むICカードにおいて、上記暗号処理用演算ユニットは、暗号化処理又は復号化処理のための演算動作と並行して次に演算の使用するデータを記憶回路から取り込む信号経路を設けることにより、演算動作とデータ転送とを同時に行なうようにすることができ、レジスタの簡素化を図りつつ電流波形を利用したアタックを無力化することができるという効果が得られる。

【0064】(4) 上記に加えて、上記暗号化処理又は復号化処理は、RSA暗号法などに応用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力されたX、Y及びNを受け、 $A=1$ 、 $B=X$ として、 $A=A^2 \bmod N$ と $A=AB \bmod N$ の演算を交互に行ない、かかる演算においてYの上位から複数ビットずつみて、上記複数ビットに対応した $A=A^2 \bmod N$ の演算を行ない、かかる演算と並行して複数ビットの組み合わせに対応した $AB \bmod N$ の演算に必要なBの値を上記記憶回路から取り込むことにより、暗号処理の高速化と機密保護とを実現できるという効果が得られる。

【0065】(5) 外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理

10

20

30

40

50

用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含む IC カードにおいて、上記記憶回路から暗号処理用演算ユニットに供給される暗号化処理又は復号化処理のためのデータは、上記記憶回路に内蔵されたアドレス発生回路に上記中央処理装置から供給された先頭アドレスを基に形成されたアドレス信号に基づいて上記暗号処理用演算ユニットにデータ転送し、かかるデータ転送に対応して上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスに乱数発生回路で形成された乱数を偽アドレス信号として送出することにより、偽アドレス信号により転送されるデータの電流波形を攪乱させることができるから、レジスタの簡素化を図りつつ電流波形を利用したアタックを無力化することができるという効果が得られる。

【0066】(6) 上記に加えて、上記暗号化処理又は復号化処理は、RSA 暗号法などに応用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力された X 、 Y 及び N を受け、 $A=1$ 、 $B=X$ として、 $A=A^2 \bmod N$ と $A=AB \bmod N$ の演算を交互に行ない、かかる演算において Y の上位から複数ビットずつみて、上記複数ビットに対応した $A=A^2 \bmod N$ の演算を行ない、上記複数ビットの組み合わせに対応して $AB \bmod N$ の演算に必要な B の値を上記記憶回路から取り込むことにより、暗号処理の高速化と機密保護とを実現できるという効果が得られる。

【0067】(7) 外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含む IC カードにおいて、上記乱数発生回路で形成された乱数を用いて上記中央処理装置において形成された暗号化されたアドレス信号を上記記憶回路に供給し、記憶回路では上記乱数を用いて上記アドレス信号を復号化して先頭アドレスを生成して暗号化処理又は復号化処理のためのデータを読み出して上記暗号処理用演算ユニットに転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスには乱数発生回路で形成された乱数が偽アドレス信号として送出することにより、記憶回路に送られるアドレス信号の読解を困難にしつつ、偽アドレス信号により転送されるデータの電流波形を攪乱させることができるから、レジスタの簡素化を図りつつ電流波形を利用したアタックを無力化することができるという効果が得られる。

【0068】(8) 上記に加えて、上記暗号化処理又は復号化処理は、RSA 暗号法などに応用可能なべき乗

剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力された X 、 Y 及び N を受け、 $A=1$ 、 $B=X$ として、 $A=A^2 \bmod N$ と $A=AB \bmod N$ の演算を交互に行ない、かかる演算において Y の上位から複数ビットずつみて、上記複数ビットに対応した $A=A^2 \bmod N$ の演算を行ない、上記複数ビットの組み合わせに対応して $AB \bmod N$ の演算に必要な B の値を上記記憶回路から取り込むことにより、暗号処理の高速化と機密保護とを実現できるという効果が得られる。

10 【0069】(9) 中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに格納することにより、演算動作の過程でのデータ転送を無くすることができるから、電流波形を利用したアタックを無力化することができるという効果が得られる。

20 【0070】(10) 上記に加えて、上記各回路を 1 つの半導体基板上において形成することにより、モジュールの小型化を図りつつ、機密保護の強化を実現することができるという効果が得られる。

【0071】(11) 中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに暗号化処理又は復号化処理のための演算動作と並行して次の演算に使用するデータを記憶回路から取り込む信号経路を設けることにより、演算動作とデータ転送とを同時に行なうようにすることができ、レジスタの簡素化を図りつつ電流波形を利用したアタックを無力化することができるという効果が得られる。

30 【0072】(12) 中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、中央処理装置により暗号化処理又は復号化処理のためのデータの先頭アドレスを上記記憶回路に供給し、記憶回路では内蔵されたアドレス発生回路により形成されたアドレス信号によりデータを読み出して上記暗号処理用演算ユニットにデータ転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスに乱数発生回路で形成された乱数が偽アドレス信号として送出することにより、偽アドレス信号により転送されるデータの電流波形を攪乱させることができるから、回路の簡素化

を図りつつ、電流波形を利用したアタックを無力化することができるという効果が得られる。

【0073】(13) 中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記中央処理装置により上記乱数発生回路で形成された乱数を用いて暗号化処理又は復号化処理のためのデータの先頭アドレスを暗号化して上記記憶回路に供給し、記憶回路では上記乱数を用いて上記アドレス信号を復号化して先頭アドレスを生成し、それを基に形成されたアドレス信号に基づいてデータを読み出して上記暗号処理用演算ユニットに転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスには乱数発生回路で形成された乱数が偽アドレス信号として送出することにより、記憶回路に送られるアドレス信号の解釈を困難にしつつ、偽アドレス信号により転送されるデータの電流波形を攪乱させることができるから、回路の簡素化を図りつつ、電流波形を利用したアタックを無力化することができるという効果が得られる。

【0074】以上本発明者よりなされた発明を実施例に基づき具体的に説明したが、本願発明は前記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば、ICカードには、1つの半導体集積回路装置を搭載するもの他、複数の半導体集積回路装置が搭載されるものであってもよい。マイクロコンピュータは、1つの半導体集積回路装置に形成されるもの他、CPUとその周辺回路が複数チップで構成されて、1つのモジュール基板上に搭載されてなるものであってもよい。

【0075】演算処理は前記のような暗号処理を行なうべき乗剰余乗算法の他に、図25図に示したフローチャート図のように演算Aと演算Bを持ち、演算Aの結果により演算Bを行なうか否かの分岐を持つような演算処理に広く利用することができる。つまり、演算Aの次に演算Bを実行し、演算Aの結果から演算Bが不要なら、その演算結果を無効にするような演算処理を行なえば、前記のような暗号処理以外の機密動作を必要とするデータ処理のハッキング対策として有益なものとなる。

【0076】上記マイクロコンピュータは、データ処理装置とかかるデータ処理装置によるデータ処理手順が書き込まれたROMを含んで記データ処理手順に従ってデータの入出力動作が行われるものであれば何であつてもよい。例えば、前記のようなICカード用チップの他に、ゲーム用等の1チップマイクロコンピュータ等のように機密保護の必要な各種マイクロコンピュータに広く適用できるものである。この発明は、機密保護を必要と

する各種ICカード及びマイクロコンピュータに広く利用できる。

【0077】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記の通りである。すなわち、外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むICカードにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータをかかえるレジスタに取り込むようにすることにより、演算動作の過程でのデータ転送を無くすることができるから、電流波形を利用したアタックを無力化することができる。

【0078】中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに格納することにより、演算動作の過程でのデータ転送を無くすることができるから、電流波形を利用したアタックを無力化することができる。

【図面の簡単な説明】

【図1】この発明が適用されるICカードの一実施例を示す外観図である。

【図2】この発明に係るICカードに搭載されるICカード用チップの一実施例を示す概略ブロック図である。

【図3】この発明に係るコプロセッサの一実施例の動作を説明するためのタイミング図である。

【図4】図3のコプロセッサの動作を説明するためのフローチャート図である。

【図5】図3のコプロセッサの一実施例を示すブロック図である。

【図6】図3のコプロセッサの他の一実施例を示すブロック図である。

【図7】図3に示したコプロセッサの動作を実現するための一実施例を示すブロック図である。

【図8】図3のコプロセッサの他の一実施例を示すブロック図である。

【図9】この発明に係るコプロセッサの他の一実施例の動作を説明するための構成図である。

【図10】図9に示したコプロセッサの動作を実現するための一実施例を示すブロック図である。

【図11】この発明に係るコプロセッサの他の一実施例の動作を説明するためのタイミング図である。

【図 12】この発明に係るコプロセッサの他の一実施例の動作を説明するためのフローチャート図である。

【図 13】この発明に係るコプロセッサの他の一実施例の動作の詳細を説明するためのタイミング図である。

【図 14】図 11 ないし図 13 に示したコプロセッサの動作を実現するための一実施例を示すブロック図である。

【図 15】この発明に係るコプロセッサの更に他の一実施例の動作を説明するためのタイミング図である。

【図 16】この発明に係るコプロセッサの演算動作の他の一実施例を示すフローチャート図である。

【図 17】この発明に係るコプロセッサの他の一実施例を示すブロック図である。

【図 18】この発明に係るコプロセッサの他の一実施例を示すブロック図である。

【図 19】この発明に係るコプロセッサの他の一実施例を示すブロック図である。

【図 20】この発明に係る IC カード用チップの他の一*

* 実施例を示す要部ブロック図である。

【図 21】図 20 のカウンタの一実施例を示すブロック図である。

【図 22】図 20 の IC カード用チップの動作の一例を示すタイミング図である。

【図 23】この発明に係る IC カード用チップの更に他の一実施例を示す要部ブロック図である。

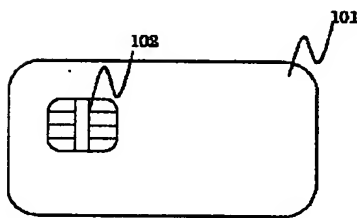
【図 24】図 23 の IC カード用チップの動作の一例を示すタイミング図である。

【図 25】この発明が適用可能な演算動作を説明するためのフローチャート図である。

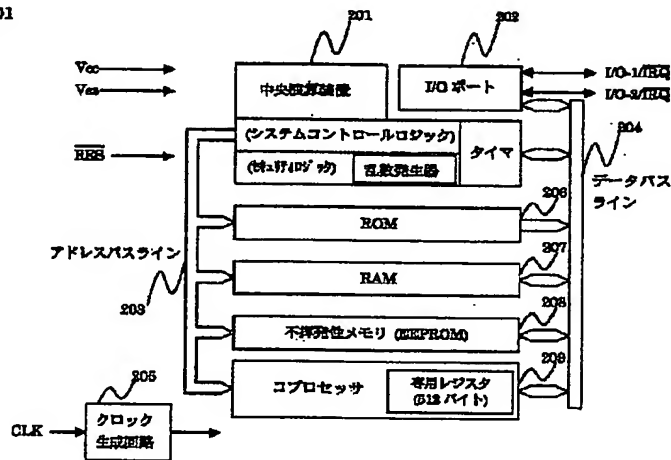
【符号の説明】

201…中央処理装置 (CPU)、202…I/Oポート、203…アドレスバス、204…データバス、205…クロック生成回路、206…ROM、207…RAM、208…EEPROM、209…コプロセッサ (暗号化処理用演算ユニット)、CDA、CDB、CDN、CDW…レジスタ。

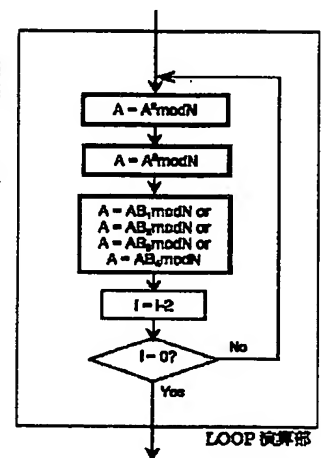
【図 1】



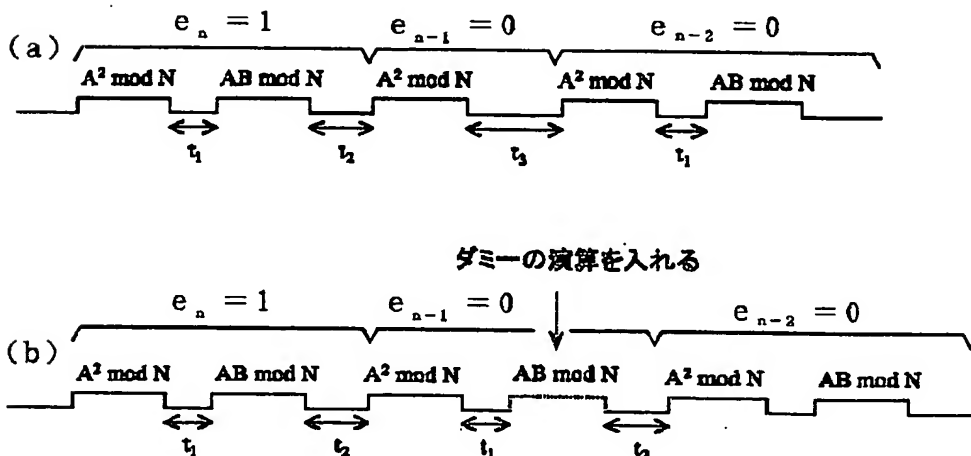
【図 2】



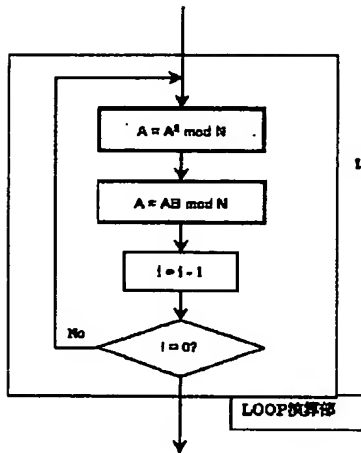
【図 16】



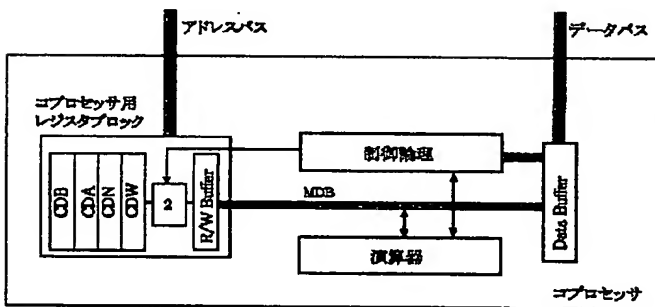
【図 3】



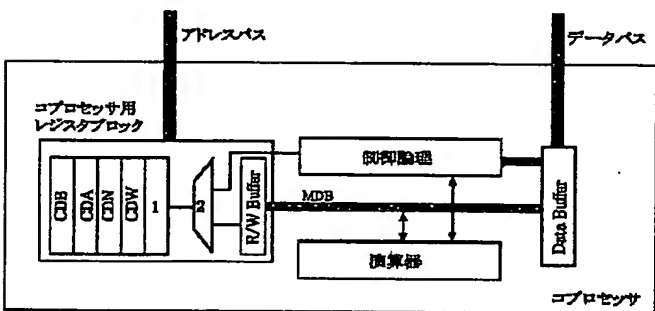
【図4】



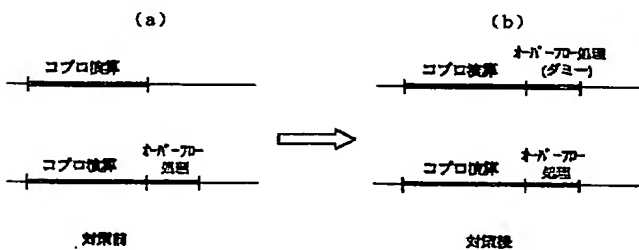
【図6】



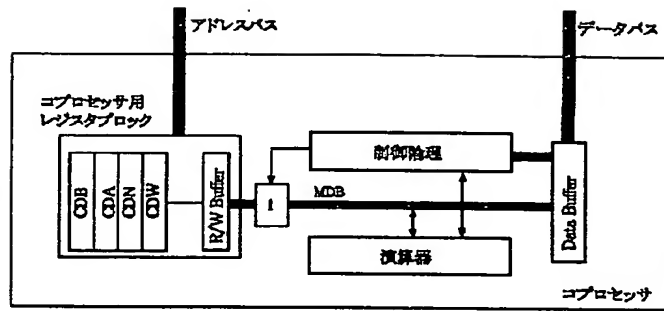
【図8】



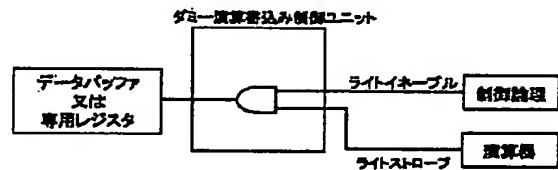
【図13】



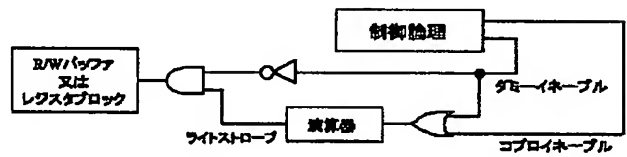
【図5】



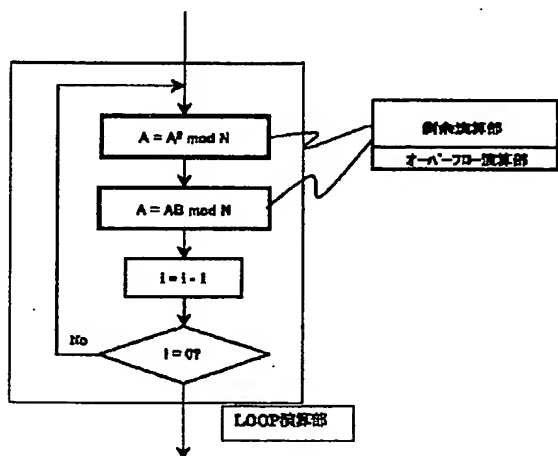
【図7】



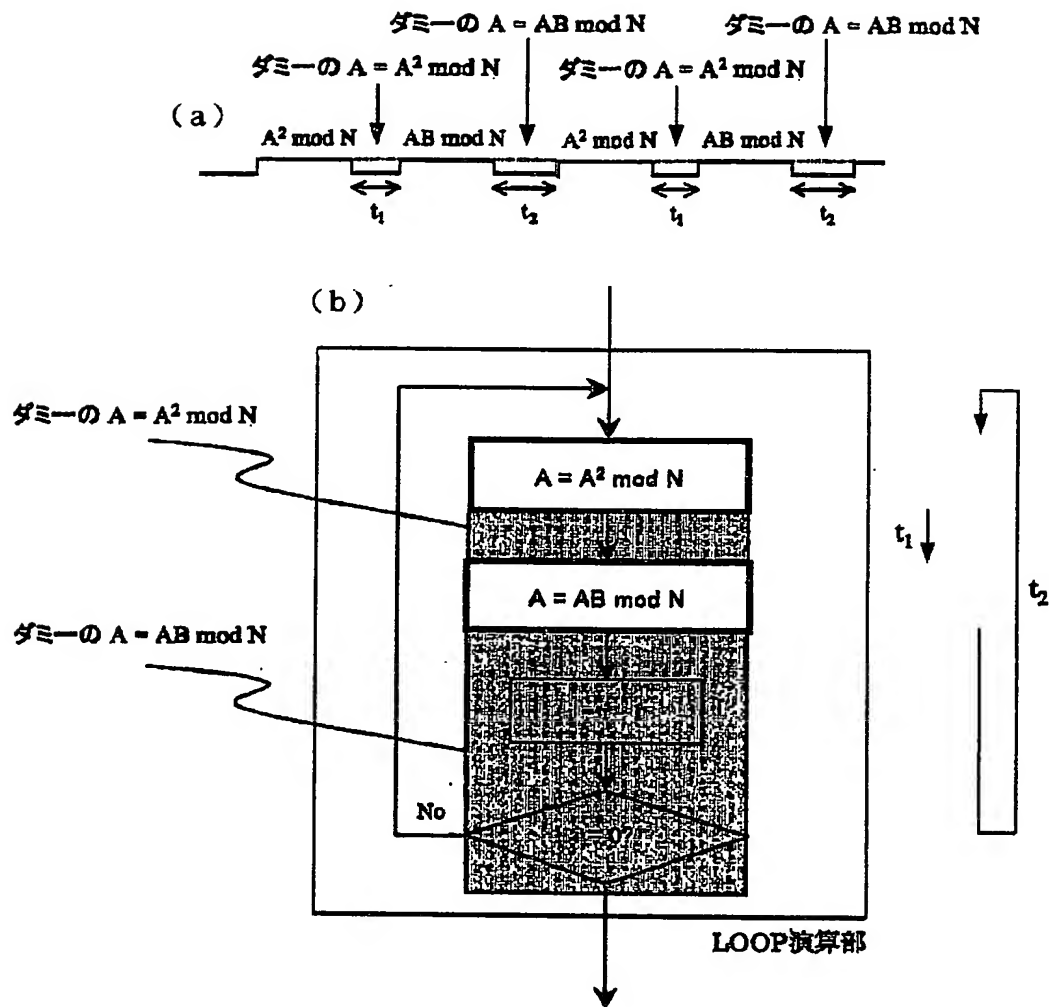
【図10】



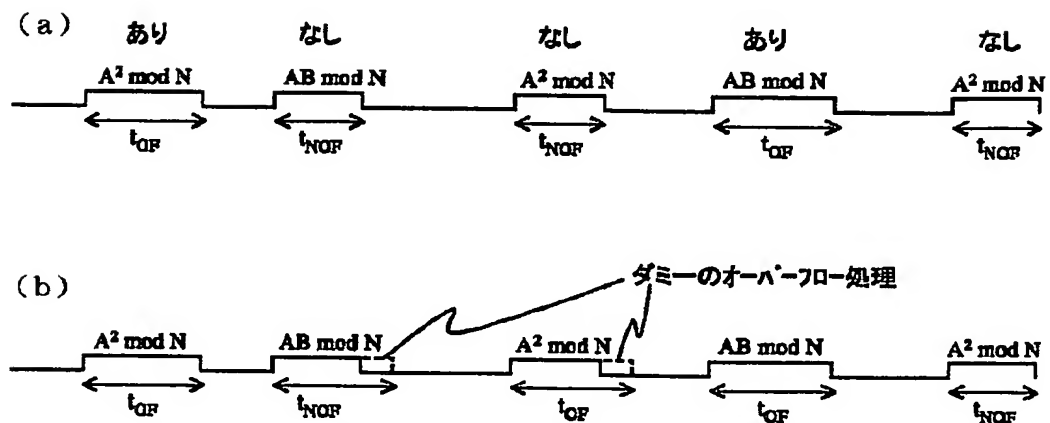
【図12】



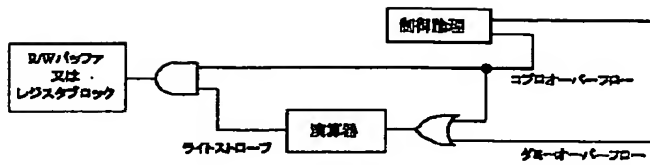
【図 9】



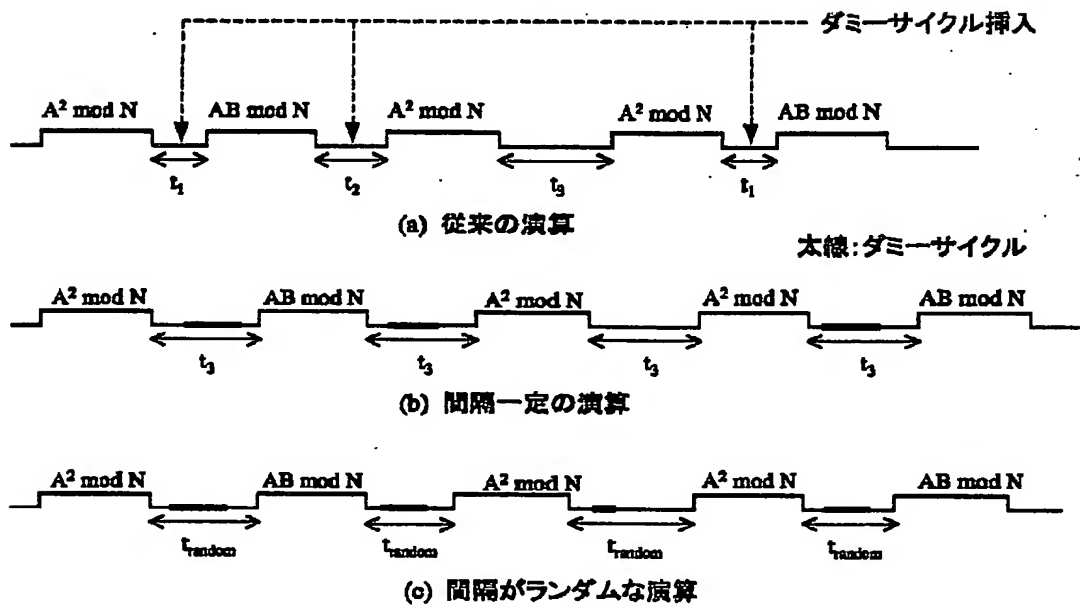
【図 11】



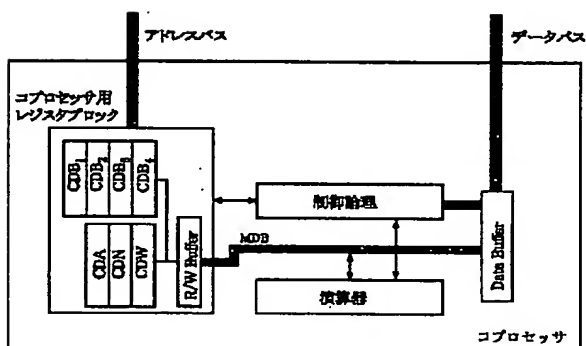
【図 14】



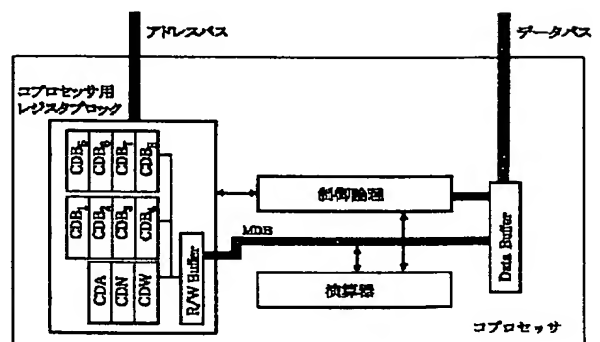
【図 15】



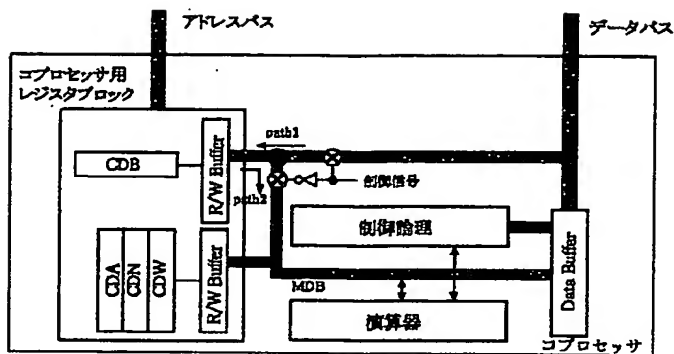
【図 17】



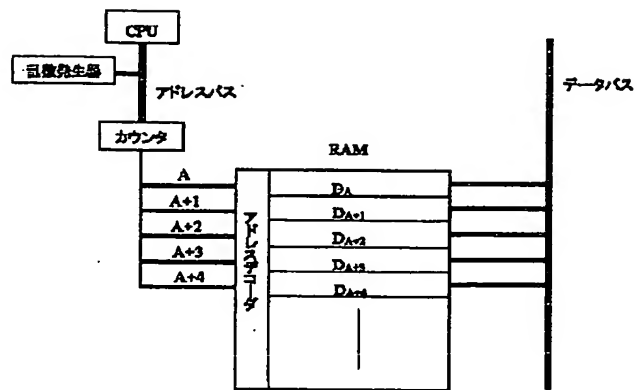
【图 18】



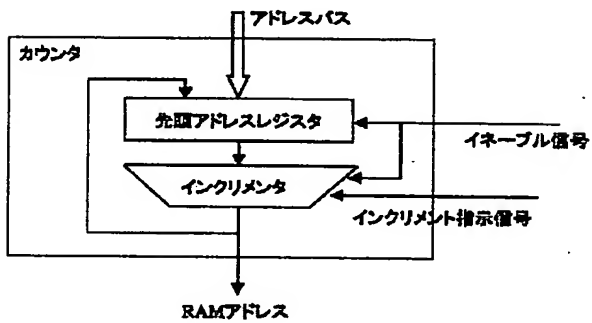
【図19】



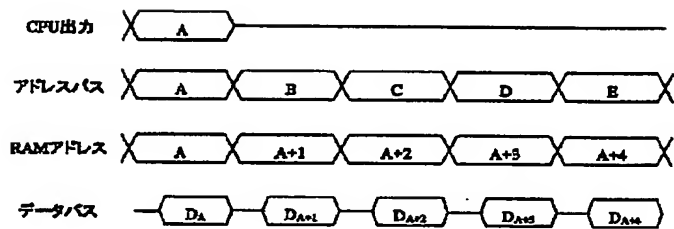
【図20】



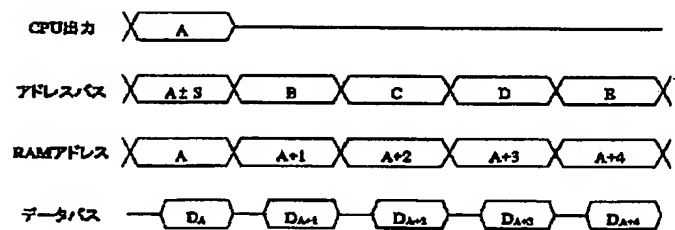
【図21】



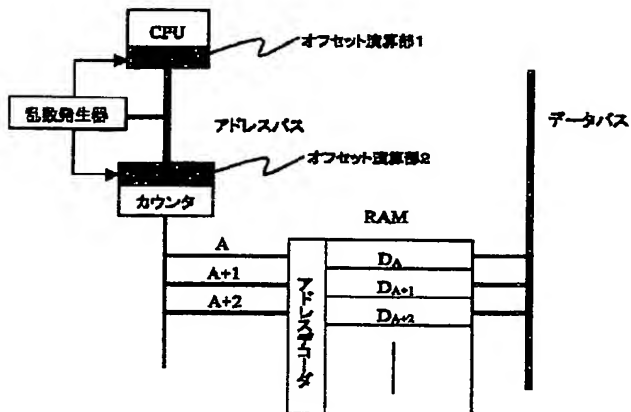
【図22】



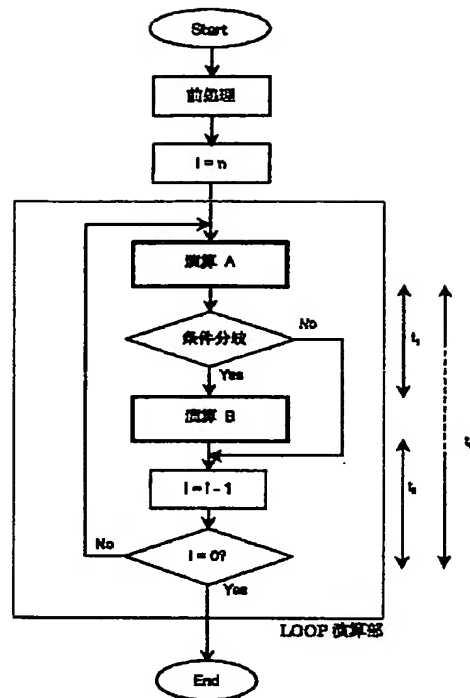
【図24】



【図23】



【図 25】



フロントページの続き

(72)発明者 中田 邦彦
 東京都小平市上水本町五丁目20番1号 株
 式会社日立製作所半導体グループ内
 (72)発明者 塚元 卓
 東京都小平市上水本町5丁目22番1号 日
 立超エル・エス・アイ・システムズ内

(72)発明者 渡瀬 弘
 東京都小平市上水本町5丁目22番1号 日
 立超エル・エス・アイ・システムズ内
 Fターム(参考) 5B017 AA03 BA07 BB09 CA14
 5B035 AA13 BB09 CA38
 5J104 AA41 JA28 NA02 NA18 NA22
 NA35 NA40
 9A001 EE03 JJ08 LL01